CLAIMS

What is claimed is:

1   1.   A method of assigning a network address to a host based on authentication for a
2   physical connection between the host and an intermediate device, the method comprising the
3   computer-implemented steps of:
4   receiving, at the intermediate device from a first server that provides authentication
5   and authorization, in response to a request for authentication for the physical
6   connection, first data indicating at least some of authentication and
7   authorization information;
8   receiving, at the intermediate device from the host, a first message for discovering a
9   logical network address for the host;
10   generating a second message based on the first message and the first data; and
11   sending the second message to a second server that provides the logical network
12   address for the host.

1   2.   A method as recited in Claim 1, wherein:
2   an authenticator process performs said step of receiving the first data;
3   a relay agent process for the second server performs said steps of receiving the first
4   message and sending the second message;
5   the relay agent process is separate from the authenticator process; and
6   said step of generating the second message further comprises the step of sending a
7   third message, from the authenticator process to the relay agent process, based
8   on the first data.

1   3.   A method as recited in Claim 1, wherein:
2   an authenticator process performs said step of receiving the first data;
3   a relay agent process for the second server performs said steps of receiving the first
4   message and sending the second message;
5   the relay agent process is separate from the authenticator process; and

-33-

6   said step of generating the second message further comprises the steps of:

7   storing second data based on the first data by the authenticator process; and

8   retrieving the second data by the relay agent process in response to said step of

9   receiving the first message.

1   4.   A method as recited in Claim 1, wherein the first server is an authentication,

2   authorization and accounting server.

1   5.   A method as recited in Claim 4, wherein the first server is a RADIUS protocol server.

1   6.   A method as recited in Claim 1, wherein the physical connection comprises an

2   Ethernet interface card on the intermediated device.

1   7.   A method as recited in Claim 1, wherein the physical connection comprises a wireless

2   Ethernet encryption key and time slot.

1   8.   A method as recited in Claim 1, wherein the request for authentication is based on an

2   Institute of Electrical and Electronics Engineers (IEEE) 802.1x standard.

1   9.   A method as recited in Claim 1, wherein the second message is based on a dynamic

2   host configuration protocol (DHCP).

1   10.   A method as recited in Claim 1, wherein:

2   the first data includes user class data indicating a particular group of one or more

3   authorized users of the host; and

4   said step of generating the second message is further based on the user class data.

1   11.   A method as recited in Claim 1, wherein:

2   the first data includes credential data indicating authentication is performed by the

3   first server; and

-34-

4   said step of generating the second message is further based on the credential data.

1 12. A method of assigning a network address to a host based on authentication for a

2 physical connection between the host and an intermediate device, the method comprising the

3 computer-implemented steps of:

4   receiving, from the host, a first request for access to a network connected to the

5   intermediate device, the first request including information about a user of the

6   host;

7   sending a second request for authentication of the physical connection to a first server

8   that provides authentication and authorization, the second request based on the

9   first request;

10   receiving, at the intermediate device from the first server in response to the second

11   request, first data indicating at least some of authentication and authorization

12   information;

13   enabling the physical connection to forward subsequent messages between the host

14   and a network connected to the intermediate device; and

15   storing the first data at least until a message is received from the host for discovering

16   a logical network address for the host.

1 13. A method of assigning a network address to a host based on authentication for a

2 physical connection between the host and an intermediate device, the method comprising the

3 computer-implemented steps of:

4   receiving, at the intermediate device from the host, a message for discovering a

5   logical network address for the host;

6   retrieving, from a persistent store at the intermediate device, first data indicating at

7   least some of authentication and authorization information received from a

8   first server that provides authentication and authorization in response to a

9   request for authentication of the physical connection;

10   generating a second message based on the first message and the first data; and

11   sending the second message to a second server that provides the logical network

12   address for the host.

1   14.   A method of assigning a network address to a host based on authentication for a

2   physical connection between the host and an intermediate device, the method comprising the

3   computer-implemented steps of:

4   receiving, from the intermediate device, a first message for discovering a logical

5   network address for the host, the first message including first data indicating at

6   least some of authentication and authorization information from a first server

7   that provides authentication and authorization in response to a request for

8   authentication for the physical connection;

9   selecting a particular pool of one or more logical network addresses, from among a

10   plurality of pools of one or more logical network addresses, based on the first

11   data; and

12   sending to the host a second message including second data indicating a particular

13   network address from the particular pool.

1   15.   A method as recited in Claim 14, wherein each pool of the plurality of pools is

2   associated with a corresponding group of a plurality of groups of one or more authorized

3   users of the host.

1   16.   A method as recited in Claim 15, wherein the first data includes user class data

2   indicating a particular group of the plurality of groups.

1   17.   A method as recited in Claim 14, wherein the particular pool is associated with a

2   privilege to access an Internet through a gateway process.

1   18.   A method of assigning a network address to a host based on authentication for a

2   physical connection between the host and an intermediate device, the method comprising the

3   computer-implemented steps of:

4   receiving, from the intermediate device, a first message for discovering a logical

5   network address for the host,

-36-

6   receiving first data from a first server that provides authentication and authorization in

7   response to a request for authentication for the physical connection, the first

8   data indicating at least some of authentication and authorization information;

9   selecting a particular pool of one or more logical network addresses, from among a

10   plurality of pools of one or more logical network addresses, based on the first

11   data; and

12   sending to the host a second message including second data indicating a particular

13   network address from the particular pool.

1   19.   A method as recited in Claim 18, further comprising the step of correlating the first

2 message and the first data.

1   20.   A method as recited in Claim 19, wherein:

2   the first message includes a unique identification for the host;

3   the first data includes the unique identification for the host; and

4   said step of correlating the first message and the first data is based on the unique

5   identification for the host.

1   21.   A method as recited in Claim 20, wherein the unique identification for the host is a

2 media access control address.

1   22.   A method of assigning a network address to a host based on authentication for a

2 physical connection between the host and an intermediate device, the method comprising the

3 computer-implemented steps of:

4   receiving, from the intermediate device at an authorization server on a network

5   connected to the intermediate device, a request for authenticating the host, the

6   request including information provided from the host;

7   determining whether the host is authentic and authorized to connect to the network

8   based on user profile data in persistent store and the request;

50325-0560 (Seq. No. 4276)

9   sending, to the intermediate device, a response indicating whether the host is authentic

10   and authorized; and

11   if it is determined that the host is authentic and authorized, then sending first data

12   based on the user profile data to a configuration server that provides a logical

13   network address for the host.

1   23.   A method of assigning a network address to a host based on authentication for a

2   physical connection between the host and an intermediate device, the method comprising the

3   computer-implemented steps of:

4   receiving, from the intermediate device at an authorization server on a network

5   connected to the intermediate device, a request for authenticating the host, the

6   request including information provided from the host for a particular user of

7   the host;

8   determining whether the particular user is authentic and authorized to connect to the

9   network based on user-profile data in persistent store and the information

10   provided from the host; and

11   if it is determined that the particular user is authentic and authorized, then sending, to

12   the intermediate device, a response indicating the host is authentic and

13   authorized,

14   wherein

15   the response includes data indicating a particular group of one or more users

16   authorized for a particular set of network operations,

17   each network operation in the particular set is controlled by a logical network

18   address of a host of a user, and

19   the group includes the particular user.

50325-0560 (Seq. No. 4276)

1   24.   A computer-readable medium carrying one or more sequences of instructions for

2   assigning a network address to a host based on authentication for a physical connection

3   between the host and an intermediate device, which instructions, when executed by one or

4   more processors, cause the one or more processors to carry out the steps of:

5   receiving, from the host, a first request for access to a network connected to the

6   intermediate device, the first request including information about a user of the

7   host;

8   sending a second request for authentication of the physical connection to a first server

9   that provides authentication and authorization, the second request based on the

10   first request;

11   receiving, at the intermediate device from the first server in response to the second

12   request, first data indicating at least some of authentication and authorization

13   information;

14   enabling the physical connection to forward subsequent messages between the host

15   and the network; and

16   storing the first data at least until a message is received from the host for discovering

17   a logical network address for the host.

1   25.   A computer-readable medium carrying one or more sequences of instructions for

2   assigning a network address to a host based on authentication for a physical connection

3   between the host and an intermediate device, which instructions, when executed by one or

4   more processors, cause the one or more processors to carry out the steps of:

5   receiving, at the intermediate device from the host, a message for discovering a

6   logical network address for the host;

7   retrieving, from a persistent store at the intermediate device, first data indicating at

8   least some of authentication and authorization information received from a

9   first server that provides authentication and authorization in response to a

10   request for authentication of the physical connection;

11   generating a second message based on the first message and the first data; and

50325-0560 (Seq. No. 4276)

12   sending the second message to a second server that provides the logical network

13   address for the host.

1   26.   An apparatus for assigning a network address to a host based on authentication for a

2   physical connection between the host and an intermediate device, comprising:

3   means for receiving, from a first server that provides authentication and authorization,

4   in response to a request for authentication for the physical connection, first

5   data indicating at least some of authentication and authorization information;

6   means for receiving, from the host, a first message for discovering a logical network

7   address for the host;

8   means for generating a second message based on the first message and the first data;

9   and

10   means for sending the second message to a second server that provides the logical

11   network address for the host.

1   27.   An apparatus for assigning a network address to a host based on authentication for a

2   physical connection between the host and an intermediate device, comprising:

3   a network interface that is coupled to a data network for receiving one or more packet

4   flows therefrom;

5   a physical connection that is coupled to the host;

6   a processor;

7   one or more stored sequences of instructions which, when executed by the processor,

8   cause the processor to carry out the steps of:

9   receiving, through the network interface from a first server that provides

10   authentication and authorization, in response to a request for

11   authentication for the physical connection, first data indicating at least

12   some of authentication and authorization information;

13   receiving, through the physical connection from the host, a first message for

14   discovering a logical network address for the host;

15   generating a second message based on the first message and the first data; and

50325-0560 (Seq. No. 4276)

16   sending through the network interface the second message to a second server

17   that provides the logical network address for the host.

50325-0560 (Seq. No. 4276)